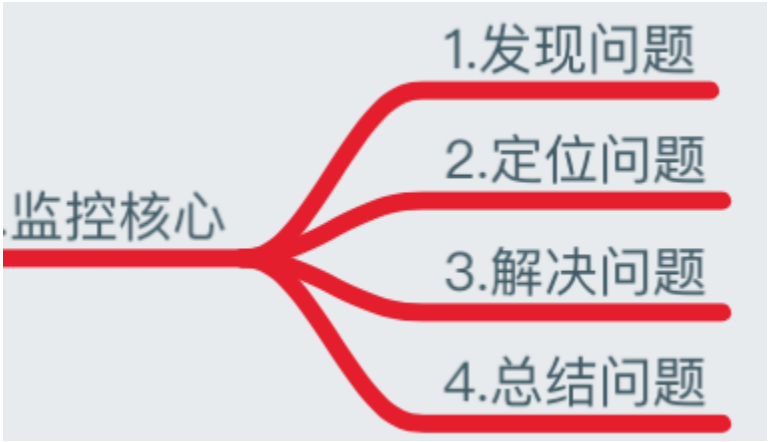
1.了解监控对象:我们要监控的对象你是否了解呢？比如CPU到底是如何工作的
2.性能基准指标:我们要监控这个东西的什么属性？比如CPU的使用率、负载、用户态、内核态、上下文切换
3.报警阈值定义:怎么样才算是故障，要报警呢？比如CPU的负载到底多少算高，用户态、内核态分别跑多少算高
4.故障处理流程:收到了故障报警，那么我们怎么处理呢？有什么更高效的处理流程吗

监控核心

我们了解了监控的方法、监控对象、性能指标、报警阈值定义、以及故障处理流程几步骤，当然我们更需要知道监控的核心是什么



1.发现问题:当系统发生故障报警，我们会收到故障报警的信息
2.定位问题:故障邮件一般都会写某某主机故障、具体故障的内容，我们需要对报警内容进行分析，比如一台服务器连不上:我们就需要考虑是网络问题、还是负载太高导致长时间无法连接，又或者某开发触发了防火墙禁止的相关策略等等，我们就需要去分析故障具体原因
3.解决问题:当然我们了解到故障的原因后，就需要通过故障解决的优先级去解决该故障
4.总结问题:当我们解决完重大故障后，需要对故障原因以及防范进行总结归纳，避免以后重复出现

监控工具

下面我们需要选择一款合适公司业务的监控工具进行监控,这里我对监控工具进行了简单的分类

老牌监控:
MRTG（Multi Route Trffic Grapher）是一套可用来绘制网络流量图的软件，由瑞士奥尔滕的Tobias Oetiker与Dave Rand所开发，以GPL授权。
MRTG最好的版本是1995年推出的，用perl语言写成，可跨平台使用，数据采集用SNMP协议，MRTG将手机到的数据通过Web页面以GIF或者PNG格式绘制出图像。

Grnglia是一个跨平台的、可扩展的、高性能的分布式监控系统，如集群和网格。它基于分层设计，使用广泛的技术，用RRDtool存储数据。具有可视化界面，适合对集群系统的自动化监控。其精心设计的数据结构和算法使得监控端到被监控端的连接开销非常低。目前已经有成千上万的集群正在使用这个监控系统，可以轻松的处理2000个节点的集群环境。

Cacti（英文含义为仙人掌）是一套基于PHP、MySQL、SNMP和RRDtool开发的网络流量监测图形分析工具，它通过snmpget来获取数据使用RRDtool绘图，但使用者无须了解RRDtool复杂的参数。提供了非常强大的数据和用户管理功能，可以指定每一个用户能查看树状结构、主机设备以及任何一张图，还可以与LDAP结合进行用户认证，同时也能自定义模板。在历史数据展示监控方面，其功能相当不错。
Cacti通过添加模板，使不同设备的监控添加具有可复用性，并且具备可自定义绘图的功能，具有强大的运算能力（数据的叠加功能）

Nagios是一个企业级监控系统，可监控服务的运行状态和网络信息等，并能监视所指定的本地或远程主机状态以及服务，同时提供异常告警通知功能等。
Nagios可运行在Linux和UNIX平台上。同时提供Web界面，以方便系统管理人员查看网络状态、各种系统问题、以及系统相关日志等
Nagios的功能侧重于监控服务的可用性，能根据监控指标状态触发告警。
目前Nagios也占领了一定的市场份额，不过Nagios并没有与时俱进，已经不能满足于多变的监控需求，架构的扩展性和使用的便捷性有待增强，其高级功能集成在商业版Nagios XI中。

Smokeping主要用于监视网络性能，包括常规的ping、www服务器性能、DNS查询性能、SSH性能等。底层也是用RRDtool做支持，特点是绘制图非常漂亮，网络丢包和延迟用颜色和阴影来标示，支持将多张图叠放在一起，其作者还开发了MRTG和RRDtll等工具。
Smokeping的站点为：http://tobi.oetiker.cn/hp

开源监控系统OpenTSDB用Hbase存储所有时序（无须采样）的数据，来构建一个分布式、可伸缩的时间序列数据库。它支持秒级数据采集，支持永久存储，可以做容量规划，并很容易地接入到现有的告警系统里。
OpenTSDB可以从大规模的集群（包括集群中的网络设备、操作系统、应用程序）中获取相应的采集指标，并进行存储、索引和服务，从而使这些数据更容易让人理解，如Web化、图形化等。

王牌监控